

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Гандич Дарья Владимировна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	12
	Список литературы	13

Список иллюстраций

3.1	Создание учетной записи guest	7
3.2	Определение директории pwd	7
3.3	whoami	7
3.4	Сравнение групп id и groups	8
3.5	Сравнение значений uid и gid	8
3.6	Существующие директории и доступные права	9
3.7	lsattr /home	9
3.8	Создание поддиректории	9
3.9	Снятие всех атрибутов	10
3.10	Создание файла	10
3.11	Таблица “УПиРД”	10
3.12	Таблица “УПиРД”	11
3.13	Таблица “УПиРД”	11
3.14	Таблица “МПДСО”	11

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

2 Теоретическое введение |

Более подробно про Unix см. в [1–4].

3 Выполнение лабораторной работы

1. Открываем ВМ, создаем учетную запись guest и задаем пароль (рис. 3.1).

```
dvgyandich login: root
Password:
Last login: Tue Feb 27 16:26:17 on tty1
[root@dvgyandich ~]# useradd guest
[root@dvgyandich ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a (reversed) dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@dvgyandich ~]# _
```

Рис. 3.1: Создание учетной записи guest

2. Определим директорию, в которой находимся с помощью команды pwd (рис. 3.2).

```
[guest@dvgyandich ~]$ cd /home
[guest@dvgyandich home]$ pwd
/home
[guest@dvgyandich home]$
```

Рис. 3.2: Определение директории pwd

3. Уточняем имя пользователя с помощью команды whoami (рис. 3.3).

```
[guest@dvgyandich home]$ whoami
guest
[guest@dvgyandich home]$ _
```

Рис. 3.3: whoami

4. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`.

Сравнивая вывод `id` с выводом команды `groups`, обнаружим, что группы, в которые входит пользователь, действительно одинаковые. Также, сравнивая вывод `id` с приглашением командной строки, обнаружим, что имя пользователя повторяется. (рис. 3.4).

```
[guest@dvgandich home]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@dvgandich home]$ groups
guest
[guest@dvgandich home]$
```

Рис. 3.4: Сравнение групп `id` и `groups`

5. Просмотрим файл `/etc/passwd` с помощью `cat /etc/passwd` и сравним данные `uid`, `gid` с результатами команд выше и выясним, что данные значения совпадают. (рис. 3.5).

```
[guest@dvgandich home]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:/usr/sbin/nologin
systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin
setroubleshoot:x:989:989:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
cockpit-ws:x:988:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-ws-instance:x:987:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:986:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
guest:x:1000:1000:/:home/guest:/bin/bash
[guest@dvgandich home]$ _
```

Рис. 3.5: Сравнение значений `uid` и `gid`

6. Определим существующие в системе директории командой `ls -l /home/`. Нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя. (рис. 3.6).


```
[guest@dvchandich home]$ ls -l /home/
total 0
drwx-----. 2 guest guest 62 Feb 29 13:02 guest
[guest@dvchandich home]$ _
```

Рис. 3.6: Существующие директории и доступные права

7. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директорий других пользователей.(рис. 3.7).

```
[guest@dvchandich home]$ lsattr /home
----- /home/guest
[guest@dvchandich home]$
```

Рис. 3.7: `lsattr /home`

8. Создаем в домашней директории поддиректорию `dir1`. Определяем командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. (рис. 3.8).

```
[guest@dvchandich ~]$ mkdir dir1
[guest@dvchandich ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 29 14:20 dir1
[guest@dvchandich ~]$ lsattr
----- ./dir1
[guest@dvchandich ~]$
```

Рис. 3.8: Создание поддиректории

9. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l` (рис. 3.9).

```
[guest@dvgyandich ~]$ chmod 000 dir1
[guest@dvgyandich ~]$ ls -l
total 0
d----- . 2 guest guest 6 Feb 29 14:20 dir1
[guest@dvgyandich ~]$ _
```

Рис. 3.9: Снятие всех атрибутов

10. Попытаемся создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 Мы получим отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверим, действительно ли файл не создавался, с помощью команды ls -l /home/guest/dir1. (рис. 3.10).

```
[guest@dvgyandich ~]$ chmod 000 dir1
[guest@dvgyandich ~]$ ls -l
total 0
d----- . 2 guest guest 6 Feb 29 14:20 dir1
[guest@dvgyandich ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@dvgyandich ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@dvgyandich ~]$ chmod 777 dir1
[guest@dvgyandich ~]$ ls -l /home/guest/dir1
total 0
[guest@dvgyandich ~]$
```

Рис. 3.10: Создание файла

11. Заполняем таблицу 2.1 “Установленные права и разрешенные действия” (рис. 3.11), (рис. 3.12), (рис. 3.13)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d----- (000)	0	-	-	-	-	-	-	-	-
d-x----- (100)	0	-	-	-	-	+	-	-	+
d-w----- (200)	0	-	-	-	-	-	-	-	-
d-wx----- (300)	0	+	+	-	-	+	-	+	+
d----- (400)	0	-	-	-	-	-	-	-	-
d-x----- (500)	0	-	-	-	-	+	-	+	+
d-w----- (600)	0	-	-	-	-	-	+	-	-
d-wx----- (700)	0	+	+	-	-	+	+	+	+
d----- (000)	-x----- (100)	-	-	-	-	-	-	-	-
d-x----- (100)	-x----- (100)	-	-	-	-	+	-	-	+
d-w----- (200)	-x----- (100)	-	-	-	-	-	-	-	-
d-wx----- (300)	-x----- (100)	+	+	-	-	+	-	+	+
d----- (400)	-x----- (100)	-	-	-	-	-	+	-	-
d-x----- (500)	-x----- (100)	-	-	-	-	+	+	-	+
d-w----- (600)	-x----- (100)	-	-	-	-	-	+	-	-
d-wx----- (700)	-x----- (100)	+	+	-	-	+	+	+	+
d----- (000)	-w----- (200)	-	-	-	-	-	-	-	-
d-x----- (100)	-w----- (200)	-	-	+	-	+	-	-	+
d-w----- (200)	-w----- (200)	-	-	-	-	-	-	-	-
d-wx----- (300)	-w----- (200)	+	+	+	-	+	-	+	+
d----- (400)	-w----- (200)	-	-	-	-	-	+	-	-
d-x----- (500)	-w----- (200)	-	-	+	-	+	+	-	+
d-w----- (600)	-w----- (200)	-	-	-	-	-	+	-	-
d-wx----- (700)	-w----- (200)	+	+	+	-	+	+	+	+

Рис. 3.11: Таблица “УПирД”

d----- (000)	-wx----- (300)	-	-	-	-	-	-	-	-
d-x----- (100)	-wx----- (300)	-	-	+	-	+	-	-	+
d-w----- (200)	-wx----- (300)	-	-	-	-	-	-	-	-
d-wx----- (300)	-wx----- (300)	+	+	+	-	+	-	+	+
d----- (400)	-wx----- (300)	-	-	-	-	-	+	-	-
d-x----- (500)	-wx----- (300)	-	-	+	-	+	+	-	+
d-w----- (600)	-wx----- (300)	-	-	-	-	-	+	-	-
d-wx----- (700)	-wx----- (300)	+	+	+	-	+	+	+	+
d----- (000)	r----- (400)	-	-	-	-	-	-	-	-
d-x----- (100)	r----- (400)	-	-	-	+	+	-	-	+
d-w----- (200)	r----- (400)	-	-	-	-	-	-	-	-
d-wx----- (300)	r----- (400)	+	+	-	+	+	-	+	+
d----- (400)	r----- (400)	-	-	-	-	-	+	-	-
d-x----- (500)	r----- (400)	-	-	-	+	+	+	-	+
d-w----- (600)	r----- (400)	-	-	-	-	-	+	-	-
d-wx----- (700)	r----- (400)	+	+	-	+	+	+	+	+
d----- (000)	r-x----- (500)	-	-	-	-	-	-	-	-
d-x----- (100)	r-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	r-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	r-x----- (500)	+	+	-	+	+	-	+	+
d----- (400)	r-x----- (500)	-	-	-	-	-	+	-	-
d-x----- (500)	r-x----- (500)	-	-	-	+	+	+	-	+
d-w----- (600)	r-x----- (500)	-	-	-	-	-	+	-	-
d-wx----- (700)	r-x----- (500)	+	+	-	+	+	+	+	+

Рис. 3.12: Таблица “УПиРД”

d----- (000)	rw----- (600)	-	-	-	-	-	-	-	-
d-x----- (100)	rw----- (600)	-	-	+	+	+	-	-	+
d-w----- (200)	rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	rw----- (600)	+	+	+	+	+	-	+	+
d----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
d-x----- (500)	rw----- (600)	-	-	+	+	+	+	-	+
d-w----- (600)	rw----- (600)	-	-	-	-	-	+	-	-
d-wx----- (700)	rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	rw-x----- (700)	-	-	-	-	-	-	-	-
d-x----- (100)	rw-x----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	rw-x----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	rw-x----- (700)	+	+	+	+	+	-	+	+
d----- (400)	rw-x----- (700)	-	-	-	-	-	+	-	-
d-x----- (500)	rw-x----- (700)	-	-	+	+	+	+	-	+
d-w----- (600)	rw-x----- (700)	-	-	-	-	-	+	-	-
d-wx----- (700)	rw-x----- (700)	+	+	+	+	+	+	+	+

Рис. 3.13: Таблица “УПиРД”

12. Заполняем таблицу 2.2 “Минимальные права для совершения операций” (рис. 3.14)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	r----- (400)
Запись в файл	d--x----- (100)	-w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Рис. 3.14: Таблица “МПДСО”

4 Выводы

Получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.